



---

On the Converse of Fermat's Theorem

Author(s): P. Erdos

Source: *The American Mathematical Monthly*, Vol. 56, No. 9 (Nov., 1949), pp. 623-624

Published by: Mathematical Association of America

Stable URL: <http://www.jstor.org/stable/2304732>

Accessed: 24/03/2010 21:39

---

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=maa>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).



Mathematical Association of America is collaborating with JSTOR to digitize, preserve and extend access to *The American Mathematical Monthly*.

<http://www.jstor.org>

## MATHEMATICAL NOTES

EDITED BY E. F. BECKENBACH, University of California, Los Angeles

*Materials for this department should be sent direct to E. F. Beckenbach, University of California, Los Angeles 24, California.*

### ON THE CONVERSE OF FERMAT'S THEOREM

P. ERDÖS, University of Illinois

Following Lehmer we shall call an integer  $n$  a *pseudoprime* if  $2^n \equiv 2 \pmod{n}$  and  $n$  is not a prime. The smallest pseudoprime is  $341 = 11 \cdot 31$ . Recently Sierpinski<sup>1</sup> gave a very simple proof that there are infinitely many pseudoprimes, by proving that if  $n$  is a pseudoprime then  $2^n - 1$  is also a pseudoprime. Lehmer<sup>2</sup> proved that there exist infinitely many pseudoprimes  $n$  with  $v(n) = 3$ , where  $v(n)$  denotes the number of different prime factors of  $n$ . In the present note we prove the following theorem.

**THEOREM.** *For every  $k$  there exist infinitely many squarefree pseudoprimes with  $v(n) = k$ .*

First we repeat Lehmer's proof<sup>3</sup> that there are infinitely many pseudoprimes  $n$  with  $v(n) = 2$ . It is well known<sup>4</sup> that for every  $m > 6$  both  $2^m - 1$  and  $2^m + 1$  have a primitive prime factor; that is, there exist primes  $p$  and  $q$  such that

$$\begin{aligned} 2^m - 1 &\equiv 0 \pmod{p}, & 2^l - 1 &\not\equiv 0 \pmod{p}, & \text{for } 1 \leq l < m; \\ 2^m + 1 &\equiv 0 \pmod{q}, & 2^l + 1 &\not\equiv 0 \pmod{q} & \text{for } 1 \leq l < m. \end{aligned}$$

It is easy to see that  $p \cdot q$  is a pseudoprime. In fact we have  $p \equiv q \equiv 1 \pmod{2m}$ ,  $2^{2m} \equiv 1 \pmod{p \cdot q}$ , thus

$$2^{2^{p-1}q-1} \equiv 2^{(p-1)(q-1)} \cdot 2^{p-1} \cdot 2^{q-1} \equiv 1 \pmod{pq}.$$

Also it is immediate that to different values of  $m$  correspond different values of  $p \cdot q$ , which proves the theorem for  $k = 2$ .

The proof of the general case will be very similar to that of Lehmer. We use induction on  $k$ . Let  $n_1 < n_2 < \dots$  be an infinite sequence of pseudoprimes with  $v(n_i) = k - 1$ . Let  $p_i$  be one of the primitive prime factors of  $2^{n_i-1} - 1$ . We claim that  $p_i \cdot n_i$  is a pseudoprime. In fact, by definition,  $2^{n_i-1} \equiv 1 \pmod{p_i \cdot n_i}$ , also  $2^{p_i-1} \equiv 1 \pmod{p_i}$ . Further, since  $p_i - 1 \equiv 0 \pmod{(n_i - 1)}$ , we have  $2^{p_i-1} \equiv 1 \pmod{n_i}$  and finally  $2^{n_i-1} \equiv 1 \pmod{n_i}$ . Thus

---

<sup>1</sup> Colloquium Math., vol. 1 (1947), p. 9.

<sup>2</sup> This MONTHLY, vol. 56 (1949) p. 306.

<sup>3</sup> This MONTHLY, vol. 43 (1936), pp. 347-356.

<sup>4</sup> Bang, Tidsskrift for Mat. 1886, pp. 130-137. See Also Birkhoff-Vandiver, Annals of Math., 1904.

$$2^{n_i p_i - 1} = 2^{(n_i - 1)(p_i - 1)} \cdot 2^{n_i - 1} \cdot 2^{p_i - 1} \equiv 1 \pmod{p_i n_i}.$$

Also  $p_i > n_i$ , since  $p_i \equiv 1 \pmod{(n_i - 1)}$  and  $n_i$  is not a prime. Thus  $p_i \cdot n_i$  is squarefree, and  $v(p_i \cdot n_i) = k$ , and all the integers  $p_i \cdot n_i$  are different; this completes the proof of the theorem.

Following Lehmer we call  $n$  an absolute pseudoprime if  $a^n \equiv a \pmod{n}$  for every  $a$  prime to  $n$ . The smallest absolute pseudoprime is 561. It seems very difficult to determine whether there are infinitely many absolute pseudoprimes. A similar question is whether there exist any composite numbers  $n$  with  $n - 1 \equiv 0 \pmod{\phi(n)}$ .

Two further questions are: Are there integers  $n$  so that  $2^n - 1$  has more than  $k$  primitive prime factors? Are there infinitely many primes  $p$  for which  $2^p - 1$  is composite? The smallest such prime is 11.

Denote by  $f(x)$  the number of pseudoprimes not exceeding  $x$ . I can prove that

$$(1) \quad c_1 \cdot \log x < f(x) < c_2 \frac{x}{(\log x)^k},$$

for every  $k$  if  $x$  is sufficiently large. In other words, the number of pseudoprimes is considerably smaller than the number of primes. The proof of (1) (second inequality) is complicated and we do not discuss it here.

#### A THEOREM ON THE DISTRIBUTION OF PRIMES

LEO MOSER, Universities of Manitoba and North Carolina

Using elementary properties of integers only, we shall establish the following result.

**THEOREM:** *For every positive integer  $r$ , there exists a prime  $p$ , with  $3 \cdot 2^{2r-1} < p < 3 \cdot 2^{2r}$ .*

This theorem is almost as strong as Bertrand's postulate, which states that for every real value of  $x \geq 1$  there is a prime  $p$  with  $x < p \leq 2x$ .

The following four lemmas follow easily from Legendre's expression for  $n!$ , namely,

$$n! = \prod_p P_{i=1}^{\infty} p^{\lfloor n/p^i \rfloor}$$

They are proved in [1], which contains an exposition of Erdős' proof of Bertrand's postulate.

(1) *If  $n < p \leq 2n$ , then  $p$  occurs exactly once in  $\binom{2n}{n}$ .*

(2) *If  $n \geq 3$  and  $2n/3 < p < n$ , then  $p$  does not occur in  $\binom{2n}{n}$ .*